

REMARKS

The Examiner objected to the drawings as not showing all of the features specified in the claims. The Examiner also required Applicant to provide descriptive text labels for all unlabeled boxes in the drawings. Applicant has amended the drawings significantly, and respectfully submits that all objections have been addressed by these amendments.

In the drawings the amendments are as follows: In Fig. 1, the unlabeled boxes have been labeled in accordance with the specification, and the lines, arrows and numbers have been drawn cleanly and uniformly. In Fig. 2, what were previously unlabeled boxes are now illustrated as the computer hardware that they are described as being in the specification, and the lines, arrows and numbers have been drawn cleanly and uniformly. In Fig. 3, the algorithm flow chart has been amended to include more descriptive text, which corresponds to the original specification and drawings. The steps “begin”, “end” and “drop packet”, which were at least implicit originally, are added. The lines, arrows and numbers have been drawn cleanly and uniformly. No new matter has been entered.

The Examiner objected to the specification as containing a hyperlink. Applicant’s attorney also noticed that a procedural error occurred by filing a translation that had been amended, but did not contain markings to indicate subject matter that was added or deleted. Therefore, included herewith are (1) the English translation of the Russian application (2) a marked-up copy of the substitute specification and (3) a clean copy of the substitute specification. The amendments made to the specification are amendments

and additions to headings, and amendments to correct minor typographical and grammatical errors in the translation. No new matter is entered.

A substitute specification showing the changes made, including removal of the hyperlink, is submitted herewith and marked CLEAN COPY OF SUBSTITUTE SPECIFICATION. A marked-up copy is submitted herewith entitled MARKED-UP COPY OF SUBSTITUTE SPECIFICATION SHOWING CHANGES MADE. The amendments to the specification address the objections and put the specification in an acceptable condition.

The Examiner rejected all claims under 35 U.S.C. §112 as being indefinite. Applicant has amended the claims to comply with §112, including making correct reference to the claim upon which each dependent claim depends. Applicant respectfully submits that the claims are now allowable under §112.

The Examiner rejected the claims 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,983,270 to Abraham (hereafter, “the Abraham reference”). The Abraham reference discloses a conventional firewall device, including a firewall 48 “which tracks and controls the flow of all data packets passing through it using the TCP/IP protocol” (see column 6, lines 6-8). However, the Abraham reference’s firewall has an address that other computers on the network can identify, and therefore use to attempt a security breach.

Applicant’s invention differs from all prior art devices, including firewalls (such as that in the Abraham reference), by the claimed network screen naming no IP or other address to the network by which the network screen is identifiable. Without an IP or

other address, the network screen is invisible to the network. This prevents attacks by avoiding access to the network screen using the network interfaces by which the network screen connects to the network. It also prevents access to the filtration rules of the network screen using the network interfaces by which the screen connects to the network. Under these circumstances, the network screen can be programmed with a set of filtration rules that it will use to control whether packets are accepted or rejected.

If it is desired to access and modify the filtration rules after the network screen is connected to the network, one embodiment of Applicant's network screen has a special control interface that is used to access and modify (also called "tune") the network screen's filtration rules. This special control interface is accessible by direct connection to the network screen through something other than the network interfaces by which the screen attaches to the filtered network. In one embodiment, this special control interface is a computer connected to a serial port or some other such control interface on the network screen.

Thus, a feature distinguishing the invention from conventional devices of this type is that the network screen is not a host of the local area network (LAN) where it is installed, and it is not involved in internetwork activity among LANs. This is because the interfaces of the claimed network screen have no logical addresses, and the MAC addresses are concealed in the course of internetwork exchange. As a result, the network screen itself is "transparent" for all types of network protocols functioning at the data link and network, and, hence, at all higher layers of the OSI model.

A transparent firewall is not taught in conventional computer networks, because firewalls are given an address in order to access the firewall using the same computer network to which the firewall is connected. The invention has a special control interface, such as a computer connected to the network screen by something other than the network which the screen is filtering, that is used to access the filtration rules. This permits modification of the filtration rules, and prevents even the possibility of an attack. Thus, the absence of physical (MAC) and network (IP) addresses of the network screen and the provision of a special control interface for transmission of control commands and setup of filtering rules are key features of the invention, and are not found anywhere in the prior art, including the Abraham reference.

The Abraham reference teaches (column 6, lines 6-8) that the “firewall server 48 [] tracks and controls the flow of all data packets passing through it [the LAN] using the TCP/IP protocol, i.e., all internet protocol or ‘IP’ packets.” A “firewall server 48” is the object of modern information security systems used in computer networks. At column 6, lines 13-17, however, Abraham teaches that “all inbound IP packet traffic from the Internet 40 passing through the firewall 48 and all outbound IP packet traffic from LAN 44 passes through a network server 50 equipped with a network operating system that coordinates this transfer of data packets.” To provide security, therefore, all outbound IP packet traffic from LAN 44 passes through the network server. Thus, network server 50 is the major link in the security system described in the Abraham reference. To transfer the security function from the firewall to a special-purpose network server 50, the latter has to be involved in internetwork activity. Therefore, the network server 50 must have

interface IP addresses assigned from the IP address block in LAN 44, where this server is installed.

The Abraham reference is further shown to be different from the claimed invention by the statement in the Abraham reference (column 7, lines 51-67) that “The filter engine 78 filters all IP packets passing through the network server 50 using the rules for each user provided by the filter executive 76.” The filter engine 78 and filter executive 76 belong to network server 50 and are in no way related to the firewall 48. Thus, the network server 50, which has at least two network interfaces (an inbound interface to connect with device 48, and an outbound one, to communicate with LAN 44), must use logical (IP) addresses of these interfaces in internetworking activities. Therefore, it is the network server 50 rather than the firewall 48 that executes packet traffic security functions in internetwork activity, a point directly indicated by the following: “IP packet may be discarded by the filter engine 78” (column 7, lines 64-65). In the claimed invention, it is the network screen (which names no address to the network) that provides the security function. This is a significant distinguishing feature of the invention.

No prior art reference has the combination of executing packet traffic security functions while having no address named to the network. This is unique to Applicant’s invention, and therefore the amended claim is distinguished from the Abraham reference and is allowable under §102. Furthermore, no reference teaches Applicant’s claimed combination of features, or suggests the combination Applicant claims. Therefore, the

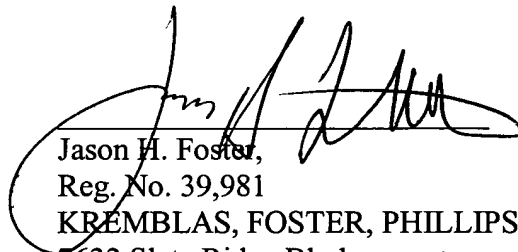
amended claims 1-7 and new claim 8 are allowable. Therefore, reconsideration and allowance are respectfully requested.

The Examiner is authorized to communicate with the undersigned attorney by email by the following recommended authorization language: Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file. (authorization pursuant to MPEP 502.03)

The Commissioner is authorized to charge Deposit Account No. 13-3393 for any insufficient fees under 37 CFR §§ 1.16 or 1.17, or credit any overpayment of fees.

Respectfully submitted,

01 November 2005
Date of Signature


Jason H. Foster,
Reg. No. 39,981
KREMBLAS, FOSTER, PHILLIPS & POLLICK
7632 Slate Ridge Blvd.
Reynoldsburg, OH 43068
Voice: 614/575-2100
Fax: 614/575-2149
email: jfoster@ohiopatent.com

Enclosures: Transmittal Form
Petition for Extension of Time
Return Receipt Postcard



1

(a) TITLE: SECURE COMPUTER NETWORK WITH A NETWORK SCREEN

Inventor: _____ Vladimir S. Zaborovskiy

Correspondence: _____

Name and Address: _____ Fractal Inc, 6748 Willow Grove Place Dublin, OH, 43017

5

(b) CROSS-REFERENCES TO RELATED APPLICATIONS

(Not Applicable)

(c) STATEMENT REGARDING FEDERALLY-SPONSORED RESEARCH AND

10

DEVELOPMENT

(Not Applicable)

(d) Reference to a "Microfiche appendix"

(Not Applicable)

15

(e) BACKGROUND OF THE INVENTION

1. Field Of The Invention

[0001] The invention relates to a computer firewall.

5

2. Description Of The Related Art

[0002] The majority of local computer networks (LCN) today have access to the Internet. However existing network protocols do not have special internal security features to secure private networks and keep data integrity. Therefore the
10 enlargement of different features and increasing requirements to the network security demand usage of special devices to block selectively information resources and control data exchange between different computer networks.

[0003] Network screens are widely used as such devices called firewalls. A network screen is a special network device that is located between two different
15 segments of an LCN in such a way that packets exchanged between these two segments is limited by special filter rules for incoming and outgoing data streams. Such a device may be installed between secured segment of an LCN and a router with one of its ports connected to the Internet. In that case filter rules of the packet traffic may block inbound and outbound activities of a secured LCN including given
20 users, time of day, days of week and months.

[0004] An example of existing firewalls is U.S. Patent No. 5,898,830, which is incorporated herein by reference, that represents a network screen located between

two computer networks with transparent network activity for the users of the secured network. For this purpose the network screen supports a configuration of two sets of virtual subscribers. The first set may be addressed only from secured segment and the second one may be addressed only from the opened segment of the network.

5 These two sets are software compatible by the table adequacy of their network addresses as it is done for DNS servers. Provisioning and restriction for the data packets from a virtual subscriber with one set of addresses to the virtual subscriber with another set of addresses is done in accordance with the rules of packets filtration that are kept in the configuration file of the network screen.

10 [0005] Virtual subscribers, except one that is especially devoted to this purpose, do not have access to the system files and other system resources of the device used as a network screen. A control program module provides configuration of the network screen and, more particularly, creation of virtual users in accordance with the configuration files written when the device was started. Access to these
15 configuration files can be provided using the rules of authorization function by a special virtual user addressed from the computer network. These rules include check of identity and authorization of the user that made a request. When this access is provided, the configuration file of the network screen that controls data exchange between computer networks may be modified. Transparency of this screen to the
20 network level protocols does not mean that this network screen cannot be discovered using special software tools. Since a set of secured network units is screened by one

network interface on the channel level of the network activity, each of these units is identified by the physical address of this network interface.

[0006] The procedure of identification of the network subscriber used to get access to the configuration file is not secured against intruders. That means the possibility of unauthorized access exists by trying different passwords or using hidden software holes.

[0007] Another known device used for similar purposes is SunScreen Secure Net 3.1 (~~www.sun.com/software/securenet~~), which is a product of Sun Microsystems. This device contains a firewall that has a so-called 'stealth mode' when no logical (IP) addresses are used for external data exchange. The SunScreen Secure Net has a network address translation function that enables a screen to map an internal network address to a different external address, masking the identity of machines within the enterprise. When packets pass between an internal host and a public network, their IP addresses are replaced with new addresses transparently, checksums and sequence numbers are corrected and the state of the address map is monitored. Administrators can specify when a packet using ordered network address translations is applied based on source or destination addresses. This device still uses physical (MAC) addresses of subscribers, for example for ARP requests for VPN tunnel functions. This means that from the inside the secured network stealth interface is completely visible.

(f) BRIEF SUMMARY OF THE INVENTION

[0008] The invention is a secure computer network with a network screen that relates generally to security engineering in a telecommunication network, ~~and,~~ and particularly to the hardware and software components of the network screens
5 (firewalls) used to block unauthorized access and data exchange between different components of the computer network.

[0009] The invention takes advantage of the capability of using the principle of the warranted security based on complete secreation of network interface addresses of a secured device. This task is resolved by using ~~the~~ a network screen that has
10 network interfaces for the data exchange between the network units but it does not have a network address. This network screen does not use network addresses for its functionality and it does not send physical addresses of the network interfaces to the external network. Therefore, this network screen cannot be located by any tools of secured or opened segments of the network.

15 [0010] According to the present invention, a special network screen is used to control filter processes of the packets traffic. This screen is completely isolated from the network interfaces that make it possible to avoid any possibility of unsanctioned access to this network screen for the users of secured and opened segments of LCN. The problem of warranted security is resolved also by the inability
20 of users of opened or secured segments of the network to create any special channel the packet data exchange between network interfaces and direct interface by means of internal system bus used for the special network screen. This special network

screen keeps information about the addresses of ~~sender~~ senders and/or ~~receiver~~ receivers using the rules of packet filtration, and makes it possible to hide the existence of the network screen from users. In other words, the filter program excludes the network screen from the list of receivers of informational packets that
 5 are coming to the network interfaces while the network screen sends the packets only to external receivers.

(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0011] This and other advantages of the invention will be apparent those of
 10 ordinary skill in the art by reference to the following detailed description and the accompanying drawings.

[0012] Fig. 1 is a general view of the network screen from the front panel side where control units and interfaces of external connections are located.

[0013] Fig. 2 is a schematic illustration of the connection between two local
 15 computing networks connected also with external network via network screen.
~~screen~~

[0014] Fig. 3 is an adapted algorithm for the program of control information that blocks ~~transmission~~ transmissions that are coming to one of the interfaces of the network screen.

20 [0015] In describing the preferred embodiment of the invention which is illustrated in the drawings, specific terminology will be resorted to for the sake of clarity. However, it is not intended that the invention be limited to the specific term

so selected and it is to be understood that each specific term includes all technical equivalents which operate in a similar manner to accomplish a similar purpose. For example, the word connected or term similar thereto are often used. They are not limited to direct connection, but include connection through other elements where
 5 such connection is recognized as being equivalent by those skilled in the art.

(h) DETAILED DESCRIPTION OF THE ~~PREFERRED EMBODIMENTS~~ INVENTION

[0016] In Fig. 1 the network screen 1 used for the local computer network
 10 (LCN) is a special computer device with internal operational system. Such a computer device may be based on a personal computers motherboard (Gigabyte, GA-5AX) that may have up to 5 external devices connected with an internal PCI bus. Such a computer device may use different types of processors including Pentium MMX, Cyrix MII, AMD K-6, RISC MIPS and others. The network screen 1 contains
 15 network interfaces for packet data exchange such as Ethernet adapters of different types with 100 Mbit/sec for ISA OR 100/10 Mbit/sec for PCI bus; for example Fast Etherlink XL 3Com.

[0017] The front panel 2 of the network screen contains connectors for 3
three data exchange interfaces, shown in Fig. 1 as reference numerals 3, 4 and 5.
 20 Each of the network adapters is connected to a local computer network segment build on the universal bus architecture with Ethernet protocol. The network screen may ~~be used~~ use up to 5 five segments of the LCN. If the LCN uses a different

protocol its network adapters should support this protocol, too. The front panel 2 also contains connectors for ~~9 and 25~~ contacts for the interfaces 6 and 7 of COM ports using standard RS232C. One of these connectors is used as an operational interface that modifies the program of control of the data exchange between segments of the LCN connected through network screen 1. The LCN segments may be connected to interfaces 3 or 4, or interfaces 3, 4 and 5 depending on their quantity. There is also a connector 8 and a source switch 9 on the panel 2. On this embodiment of the invention network screen 1 ~~has~~ uses the operating~~operational~~ system UNIX that provides multitask functionality for the program of control in accordance with a configuration file that is located in source undependable memory device of the network screen 1.

[0018] In Fig. 2 is shown an example of a connection between the LCN and the network screen 1. Network screen 1 there splits a secured corporate LCN 10 with bus architecture into segments 11, 12 and 13, which are connected, respectively, to the network adapters 3, 4 and 5. Such a structure of LCN 10 may be used in the corporate computer network where different network segments are used for different types of data applications. These applications may have different requirements for the level of confidentiality of delivered data that is taken into consideration for each of the network interfaces.

[0019] ~~On~~ In this example segment 13 contains only one subscriber, gate 14, that provides connection of the LCN 10 with an external network 15. The network 15 may be connected with the other network also. The gate 14 can use modem lines to

connect the LCN with the Internet using dial-up channels. Each of the segments 11 and 12 of the LCN contains several subscribers 16 and 17 that are connected to these network segments by the Ethernet adapter 18. To make changes in the program of control network packets delivery between interfaces 3, 4 and 5 including filter rules, a special computer 19 is connected to control interface 6. These modifications of the control program may be done from the computer 19 using a standard program of a Web navigator (browser), for example Netscape Navigator, using a connection between computer 19 and network screen 1 authorized with password by protocol PPP.

10 [0020] The program of control provides network packets delivery between the network interfaces that are addressed to the users of opened or secured segments. Since the network screen does not have addresses associated with its network interfaces, this screen cannot be used as a receiver of any network packets, it can be used only as a passive transit unit between network interfaces or as a breaker that rejects packets that did not pass filter rules between these interfaces. The program of control network packets delivery for interfaces 3, 4 and 5 (driver of the network adapters Ethernet) keeps unchanged address filed of sender in their information blocks that are delivered to the network screen 1 through interfaces 3, 4 and 5.

[0021] The gate 14 works as a router that exchanges information about conditions of the network connections with another device of the same kind and sends packet traffic to the other segments of the corporate network and to the Internet. Therefore, the LCN 10 is completely secured by the network screen with

network interfaces that do not have physical (MAC) and logical (IP) addresses. Such a screen is untouchable for remote attacks through computer networks because it is not a receiver of the information packets. The network screen cannot be detected by standard tools of network identification because its interfaces used for connections
5 with network segments are operated in such a way that they do not answer for ARP requests about their physical (MAC) addresses.

[0022] Fig. 3 shows an algorithm of filter packets coming to the network interface 5. Each packet coming through the segment 11 of LCN 10 receives by ~~interface~~interfaces 5 that keep it in its buffer memory. Primary processing of it
10 according to the filter rules consists of a sequential execution of the operations 20 and 21 that is a sequential test of receivers physical address Ad in the header of the processing packet.

[0023] While certain preferred embodiments of the present invention have been disclosed in detail, it is to be understood that various modifications may be
15 adopted without departing from the spirit of the invention or scope of the following claims.

ABSTRACT OF THE DISCLOSURE

This invention takes advantage of the capability to keep secured physical and logical addresses of the internal subscribers of the local network using a special network screen for the packets exchanged between the network segments and using a special program to control the packets communication processes between the network interfaces.

- 5 The program of control resolves the task of information delivery using special codes in the packet headers that are different from their logical and physical addresses. The network screen has a special interface to change, control and tune filter parameters.